SOLUTION BRIEF

Illumio for IBM z/OS, Powered by BMC

Illumio and BMC make Zero Trust security a reality for mainframes

Challenges in Securing Mainframe Environments

The mainframe is the backbone of enterprises worldwide, running critical applications and storing mission-critical data.

However, in many environments, the mainframe communicates with workloads in the data center and cloud. Many organizations lack a cohesive view of traffic flows from mainframe to data center and cloud workloads and the ability to extend Zero Trust security policies across these environments.

These security gaps leave the mainframe open to potentially devastating breaches, creating opportunities for attackers to move laterally and gain access to applications and underlying data.

What's more, a common challenge is integrating the mainframe with the enterprise security framework. Whether these solutions support IAM, PAM or certificate management functions, the mainframe is often left out of the implementation due to compatibility challenges.

Organizations need to prioritize adopting a Zero Trust framework to secure mainframes and protect their most sensitive data.

Modernizing Mainframe Security With Full Visibility and Zero Trust Control

Illumio and BMC have partnered to bring the only Zero Trust Segmentation solution to market that covers the breadth of platforms needed to secure the modern enterprise.

BMC AMI Enterprise Connector for Illumio (eC for Illumio) connects IBM mainframe systems to enterprise solutions, solving network connectivity and data compatibility challenges.

eC for Illumio provides two key services:

- eC for Illumio adds IBM z/OS service visibility to Illumio's application dependency maps. This visibility provides mainframe administrators and security teams with the insight needed to create targeted Zero Trust security policies inclusive of z/OS, distributed systems and cloud workloads.
- eC for Illumio sets security policies in the native mainframe IP controls to ensure that only allowed connections are permitted.

With eC for Illumio, organizations can easily bring Zero Trust security to the mainframe and remain resilient in the face of rising cyber threats.

Why Is Zero Trust Important for Mainframes?

Safeguard your most important assets and services on IBM z/OS with Zero Trust security controls from Illumio and BMC

See Risks
Gain continuous visibility and insights into traffic across servers, applications, devices, geographies and more.

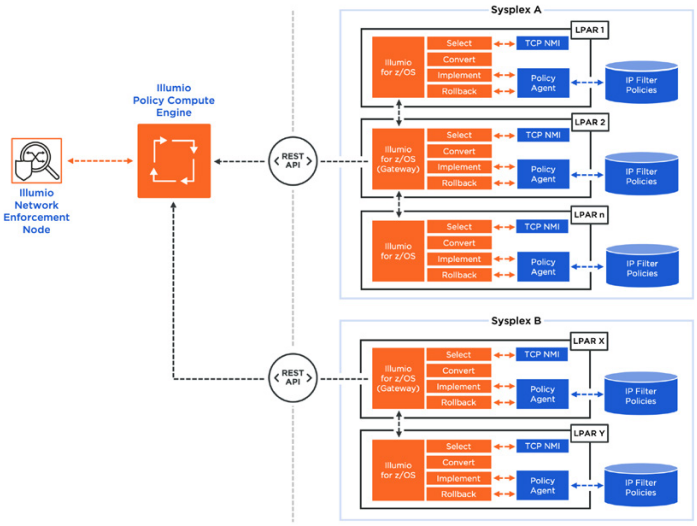
Isolate Attacks
Easily apply automated Zero Trust Segmentation policies and eliminate the risk of unauthorized access.

Secure Data
Secure data-in-transit without requiring any changes to existing infrastructure or sacrificing performance.

Illumio and BMC Joint Solution: How It Works

Here's how eC for Illumio works using two fictional sysplex for simplicity. In practice, customer sites may have more logical partitions (LPARs).

The following diagram outlines the high-level eC for Illumio architecture.



eC for Illumio acts as the interface between Illumio Core and the IBM Z Series. It is installed as a z/OS resident application and communicates with the Illumio Policy Control Engine (PCE).

The Illumio PCE collects network data from the mainframe and then implements a wide range of network security policies known as Access Control Lists (ACLs).

eC for Illumio provides z/OS support for a subset of these ACLs that enforce Zero Trust on the mainframe.

Key Capabilities

Every eC for Illumio instance will perform the following processes:

- Extract static and dynamic interface addresses for the LPAR using IBM NMI APIs.
- Select the ACLs that match the interface addresses for the LPAR.
- Determine whether the policies have changed since the last download.

If the policies have changed:

- Convert the ACL format from the PCE to the IBM Policy Agent configuration format.
- Read the existing Policy Agent configuration and merge the PCE-supplied policies.
- Generate availability notification of a new policy.

Support implementation:

- Provide user command/interface to activate new policy for the Policy Agent.
- Provide user command/interface to activate a previous policy (rollback).
- Write a full audit log of all activity.

Contact us today to learn more about how to make mainframe Zero Trust a reality with eC for Illumio.

Visit: illumio.com/contact-sales

About Illumio

Illumio is the leader of Zero Trust Segmentation. See your risks, isolate attacks and secure your data to stop breaches from becoming cyber disasters.

About BMC

From core to cloud to edge, BMC delivers industry-leading mainframe transformation solutions and helps organizations thrive in the midst of disruption by securing and integrating their mainframe into enterprise security platforms.